The “three M’s” counter-measures to children’s risky online behaviours: mentor, mitigate and monitor

Karen Renaud
Suzanne Prior

This author accepted manuscript is deposited under a Creative Commons Attribution Non-commercial 4.0 International (CC BY-NC) licence. This means that anyone may distribute, adapt, and build upon the work for non-commercial purposes, subject to full attribution. If you wish to use this manuscript for commercial purposes, please contact permissions@emerald.com

Renaud, K. & Prior, S. (2021) 'The “three M’s” counter-measures to children’s risky online behaviours: mentor, mitigate and monitor'. *Information and Computer Security*. DOI: 10.1108/ICS-07-2020-0115

The "Three M's" Counter-Measures to Children's Risky Online Behaviours: Mentor, Mitigate and Monitor

Journal:	*Information and Computer Security*
Manuscript ID	ICS-07-2020-0115.R4
Manuscript Type:	Original Article
Keywords:	Cybersecurity, Cybersafety, Children, Online Harms, Visualisation

SCHOLARONE™
Manuscripts

The "Three M's" Counter-Measures to Children's Risky Online Behaviours: *Mentor*, *Mitigate* and *Monitor*

Karen Renaud, University of Strathclyde, Scotland. karen.renaud@strath.ac.uk
Suzanne Prior, Abertay University, Scotland. s.prior@abertay.ac.uk

Design/methodology/approach

With children increasingly operating as independent agents online, their teachers and carers need to understand the risks of their new playground and the range of risk management strategies they can deploy. Carers and teachers play a prominent role in applying the three M's: *mentoring* the child, *mitigating* harms using a variety of technologies (where possible), and *monitoring* the child's online activities to ensure their cybersecurity and cybersafety. In this space, the core concepts of 'cybersafety' and 'cybersecurity' are substantively different, and this should be acknowledged for the full range of counter-measures to be appreciated. Evidence of core concept conflation emerged, confirming the need for a resource pack to improve comprehension. A carefully crafted resource pack was developed to convey knowledge of risky behaviours for three age groups, and mapped to the appropriate "three M's" to be used as counter-measures.

Purpose

To scope the field of child-related online harms and to produce a resource pack to communicate all the different dimensions of this domain to teachers and carers.

Findings

The investigation revealed key concept conflation, then identified a wide range of harms and countermeasures. The resource pack brings clarity to this domain for all stakeholders.

Limitations

The number of people who were involved in the empirical investigation were limited to those living in Scotland and Nigeria, but it is unlikely that the situation is different elsewhere, because the Internet is global, and children's risky behaviours are likely to be similar across the globe.

Originality

Others have investigated this domain but no one, to our knowledge, has come up with the "Three M's" formulation and a visualisation-based resource pack that can inform educators and carers in terms of actions they can take to address the harms.

KEYWORDS

Cybersafety, Cybersecurity, Online Risky Behaviours, Age Groups, Countermeasures

Information and Computer Security

1. Introduction

Children are accessing Internet services, on average, from 4.9 years of age (Wayman, 2017) and using it extensively for a variety of purposes (Clarke, 2002). UNICEF (2019) estimates that 71% of the world's children are active online. While the Internet is a wonderful resource, it is not necessarily a safe or secure space for children to explore (Wilson, 2020). Hackers and online predators populate the online world (Her Majesty's Government, 2019), and every online user has to practice cybersecurity and cybersafety, with the latter being particularly important for young children. Grainia Long, the chief executive of the Irish Society for the Prevention of Cruelty to Children (ISPCC), warns that cybersafety is "*the child protection issue of our time*" (Kennedy, 2016).

Children should be made aware of cybersecurity principles (Alotaibi, Furnell, Stengel, and Papadaki, 2016) and also understand how to preserve their own cybersafety (Edwards, Nolan, Henderson, Mantilla, Plowman, and Skouteris, 2018, Heider, 2015a, Edwards, Nolan, Henderson, Skouteris, Mantilla, Lambert, and Bird, 2016a; Livingstone and Bober, 2004). Given their tender years, many measures have to be implemented by the adults in the children's lives – similar to the way parents apply measures in the physical world to keep their children safe and secure. Adults have a prominent role to play in preparing children for a future where they will operate unchaperoned, as increasingly independent agents in the online world (Pietre-Cambacédes and Chaudet, 2010).

Many parents are very concerned about their children seeing harmful content online (Ofcom, 2020). Yet, parents are not necessarily aware of the full range of online harms nor of the counter measures they can implement (Symons, Ponnet, Emmery, Walrave, and Heirman, 2017; Livingstone, Mascheroni, Ólafsson and Haddon, 2014; Davis et al., 2019). Livingstone, Davidson and Bryce (2017) explain that "*gaps remain in parents' abilities and skills for effective mediation; rules and restrictions tend to keep children safe but constrain their opportunities and invite evasion*" (p. 4). Teachers, too, need more support (Berson and Berson, 2003; Green, Wilkins and Wyld, 2019).

Thomas Jefferson is reported to have said: "*If we think [the people] are not enlightened enough to exercise their control with a wholesome discretion, the remedy is not to take it from them, but to inform their discretion*" (quoted by William Ruckelshaus, 1983, p. 1027). There is thus a need to provide parents and teachers with more resources to inform them (Annansingh and Veli, 2016).

Section 2 reviews related research. Section 3 provides the research question and the aims of this research. Section 4 lays out the research methodology, and Section 5 reports on the research conducted to confirm the need for the proposed resource. Section 6 scopes the core concepts to be communicated and Section 7 explains how the visualisation and resource pack were derived and produced. Section 8 discusses and reflects on the research and Section 9 concludes.

Information and Computer Security

2. Background and Related Research

Given that Article 17 and 19 of the UN Convention on the Rights of the Child state that the role of government is to exercise due diligence in terms of protecting its children (Walker, 2017), the UK government's stance in this respect will be considered. The UK government recently released an Online Harms White Paper (Her Majesty's Government, 2019). The white paper discusses a range of online harms and says that it aims to "*put forward ambitious plans for a new system of accountability and oversight for tech companies, moving far beyond self-regulation*" (p. 3). They are, understandably, starting off by ensuring that the necessary regulatory frameworks are in place, and communicating this to relevant industries. The International Telecommunications Union (2020) also released a white paper titled "Guidelines for industry on Child Protection", and UNICEF (2014) published guidelines titled "Guidelines for Industry on Child Online Protection". These, like the UK government's white paper, target industry audiences.

A number of bodies are dedicated to formulating youth online safety programmes (e.g., Be Internet Awesome and Cybercivics). Finkelhor, Walsh, Jones, Mitchell and Collier (2020) examined the messages formulated by these, and discovered that many of the messages, especially those related to sexual exploitation and sexting, were suboptimal. Their review includes cybersecurity (e.g., hacking) and cybersafety (e.g., cyberbullying) harms, although the title refers only to safety. These bodies target institutions that construct prevention-related education programmes, not individual parents and teachers.

What about academic research? Some researchers address specific cybersafety issues, such as sexual exploitation (Quayle, 2020), the impact of pornography on young adolescents (Martellozzo, Monaghan, Davidson, and Adler, 2020), cyberbullying (Franco and Ghanayim, 2019; Martzoukou, 2020) and the extent of the harms experienced by children online (Slavtcheva-Petkova, Nash and Bulger, 2015). While these are excellent papers, they are not intended to provide an overview of the online harm domain.

Parents seeking advice about a range of issues use search engines to search for guidance (Moseley, Freed, and Goold, 2011). A search of the online domain for harm-related guidance rendered some guidelines, but these were not comprehensive nor were they presented in an easy-to-process format. The narrow focus and often outdated advice issue are highlighted by Green, Wilkins and Wyld (2019). For example, Ben-Joseph (2018) publishes guidelines for parents, but the list does not include a number of pertinent cybersecurity-related online harms (password good practice). The ThinkUKnow website (undated-b) provides a link to GOV.UK (2019), which provides curriculum advice for teachers. The list of harms they provide includes cybersafety (misinformation), cybersecurity (password phishing) and cyberprivacy (personal data), but is not exhaustive (e.g., children hacking is

Information and Computer Security

not mentioned although the UK government has a programme to address this[1]). The focus is on education, which is understandable. As such, it does not introduce technical measures that could be deployed by adult stakeholders to address harms. Here, too, there is no classification of risky behaviours according to the ages at which children might engage in potentially harmful online activities of each type. Finally, the NSPCC provides advice for parents in terms of understanding and addressing online safety related harms. This is an excellent resource but does not include any cybersecurity advice.

Tambini (2019) criticises the UK government's White Paper, arguing that the harms are insufficiently defined, and Nash (2019) concurs. The Child Rights Online Network (2019) criticise the fact that "*the White Paper does not provide a definition of the term or set the scope of its application*" (p. 1). These criticisms confirm the need for more clarity in this domain. Moreover, none of the reviewed sources consolidate both cybersafety and cybersecurity harms and counter-measures into an easily accessible format for parents and teachers. The target audience of this research project is teachers, firstly, and then parents as future work. The aim is to empower these stakeholders by satisfying their need for a concise and understandable overview of the domain, including the actions they can take to protect the children in their care.

3. Research Questions and Aims

At the 28th session of the Human Rights Council, Monday 9 March 2015 (United Nations, 2015). Special Representative of the UN Secretary-General on Violence against Children, Tomas Lamanauskas argued for the importance of engaging and empowering children, parents and teachers in this space, which is what this research aims to achieve. Adults and teachers are referred to as "adult stakeholders" in this paper.

The research question is:

> *How best can adult stakeholders be helped to understand the full range of risky online behaviours and the appropriate countermeasures that they can take to prevent online harms to the children in their care?*

The stages engaged in to answer the research question are as follows:

1: **Confirm lack of understanding:** Define the two core cyber terms and then ascertain whether the various stakeholder groups distinguish between them. Crucially, to determine

[1] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyberchoices

Information and Computer Security

whether they make a distinction between the assurance measures that are taken in these two areas.

2: **Scope the domain (*identify the full range of behaviours*):** Identify the full range of risky online behaviours that children are likely to engage in, the ages at which they might engage in these. Then, to map them to the associated counter measures that can be taken to ameliorate them.

3: **Develop an appropriate way to help them (*how best*):** Develop a resource pack to transfer the knowledge to stakeholders. This should communicate the risks and counter measures in an accessible and understandable format.

4. Research Methodology

The research choices can be characterised according to Saunders, Lewis and Thornhill (2016)'s research onion:

- *Philosophy*: Interpretivist (sub-question 1) and positivist (sub-questions 2 & 3).
- *Approach to Theory Development*: Abductive (explore a phenomenon, identify themes and patterns, collect more data and so forth).
- *Methodological Choice*: Mixed method (at least one quantitative and at least one qualitative (Cresswell, 1999)).
- *Strategies*: Survey, Systematic Literature Review, Desk Research, Focus Groups, Expert Review.
- *Time Horizon*: cross-sectional snapshot.
- *Techniques and Procedures*: collecting primary data and carrying out open coding analysis, systematically reviewing literature, harvesting secondary data, designing and refining visualisation.

When a researcher has a specific hypothesis, a positivist research philosophy can reveal general laws of behaviours and the causal relationships within the research space (Crotty, 1998). Yet, Crotty explains that when there is a need to understand how people *construct meaning*, more interpretivist approaches need to be used. Saunders et al. (2016) explain that a purely positivist approach (i.e., hypothesis led) does not afford a rich and nuanced view of reality and does not reveal differences in individual experiences.

Hence, in terms of addressing research sub-question (1), a combination of a systematic literature review and an interpretivist approach was used. The former gathered relevant research publications to reveal academic usage of the key terms (Section 5.1), and the latter revealed the meanings laypeople have constructed related to the two key terms (Section 5.2: teachers, Section 5.3: secondary school

Information and Computer Security

students and 5.4: primary school pupils). The mixed methods approach was indicated because, as argued by Morse (2016), it was necessary to explore the issue of online harms from different perspectives and levels (Figure 1 provides an overview.)

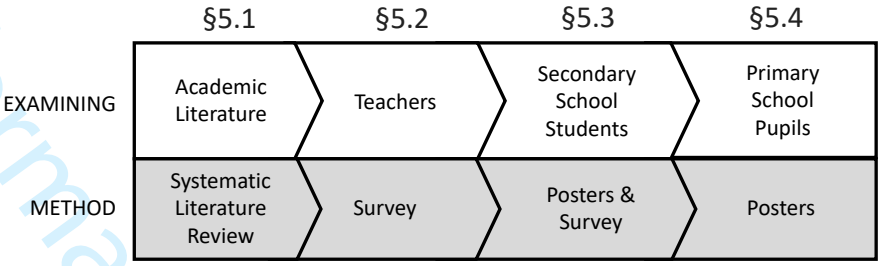

Figure 1: Methodology for Sub Question 1.

To address research sub-question (2), desk research was used. Bednarowska (2015) argues that this kind of research is somewhat neglected but has particular power in terms of gathering facts and existing research publications from secondary data sources. It allows a researcher to use a wide range of sources to gather information about a specific topic. This was deemed the best way to ensure that a comprehensive list of child-specific risky online behaviours and related counter measures was compiled, especially since much of the work in this area appears in the grey literature. Using desk research allowed us to link these publications to relevant peer-reviewed papers to ensure that an exhaustive a list as possible was compiled, as outlined in Section 6. We conducted focus groups with trainee teachers to help to verify the comprehensiveness of the list, and augmented it accordingly, as outlined in Section 6.1.1. The ages at which children were likely to engage in these behaviours, and the counter measures that could be used to address them, were also identified using desk research.

A validation process, using a webinar, helped to confirm the comprehensiveness of the harms and counter measures, as outlined in Section 6.4, Each risky behaviour, in turn, was presented and participants were asked to provide feedback on the counter-measures. At the end, participants were asked whether any relevant risky behaviours had been omitted. They provided feedback via an anonymous Google form (Figure 2 provides an overview).

Information and Computer Security

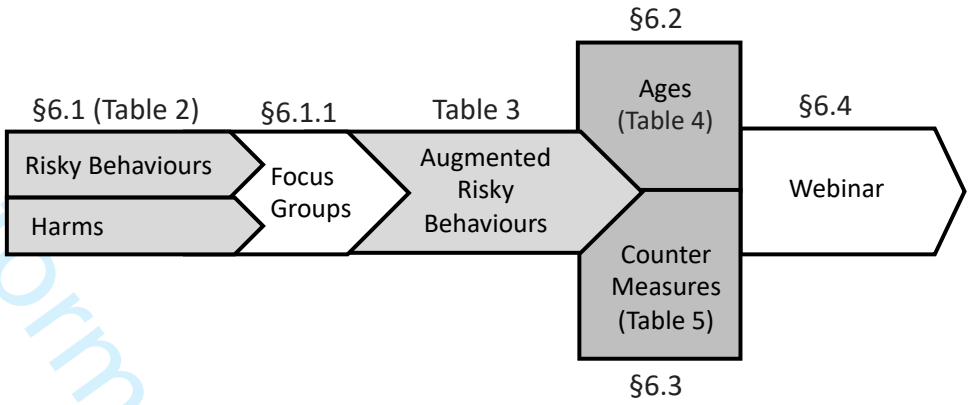

Figure 2: Methodology for Sub Question 2.

To address research sub-question (3), Section 7 motivates the use of a visualisation instead of text to communicate domain knowledge. Renaud and Van Biljon (2019) recommend assessing their *communicative power*. Experts were recruited to help to ensure: (1) comprehensiveness of risky behaviours, and (2) appropriateness of the counter measures, as described in Section 7.2 (Figure 3 provides an overview.)

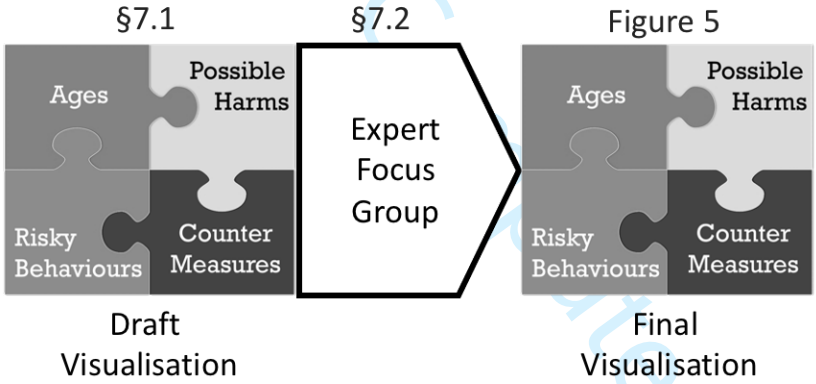

Figure 3: Methodology for Sub Question 3.

4.1 Sampling

Convenience sampling was used to support the investigations. This technique involves selecting cases because they are available (or feasible) to obtain (Saunders et al., 2016).

To answer the first sub-question, the understandings of three groups needed to be gauged: teachers, secondary school students and primary school pupils. For teachers, a survey was published specifically to gather teacher responses online, and teachers recruited via University and personal

Information and Computer Security

contacts, to reveal their understanding of the core terms. After removing unusable and nonsense responses from the 95 in total, 56 usable responses were retained for analysis.

To gauge understanding of core terms by the secondary school students, responses were gathered from 13-14 year old students participating in a University-hosted event. The secondary school students came from a variety of secondary schools and the outreach event was organised by the University's external relations department. Before the lecture (to ensure that responses were not framed), they created a poster (in groups) about password good practice and completed a survey. They then received a lesson on password good practice. Fifty students attended the session. Eleven group posters and 35 survey responses were collected.

Third, primary schools within reach of the author's University were contacted. Four schools were visited to gather insights from 8-9 year-old children. A3 sized paper sheets, crayons and stickers were provided and children were asked to make posters about password good practice. They then received a lesson on creating good passwords. 8-9 year-olds were targeted, because they are generally literate and able to write simple words and sentences without assistance. A hundred and forty-one anonymous posters were collected from 142 children in the four schools.

A comprehensive list of online harms and counter measures was compiled from the research and gray literature. Trainee teachers were recruited to review the list via the local teacher training college. Six separate focus groups were conducted online with eleven trainee teachers in total going through the list of harms to give their opinions as to the comprehensiveness and correctness thereof. After revising the list of harms, the mapping of harms to countermeasures was presented to a focus group for evaluation by 98 Nigerian participants during a webinar. Each harm was presented, with its countermeasures, and they were asked to provide feedback. Thirteen responses were received via an anonymous Google form.

Having validated the list of harms, the visualisation was produced. Experts were recruited to evaluate it, including: two secondary school teachers, a CISO and ten cybersecurity experts from the authors' institution, which has a cyber security division.

The webinar, and focus groups were conducted online due to the pandemic.

4.2 Data Collection & Analysis

Data was collected via posters (children, both primary and secondary school) and surveys (teachers and secondary school students). Expert responses were collected via focus groups, with both authors taking notes.

Information and Computer Security

The posters produced by primary school pupils and secondary school students were qualitatively analysed using Content Analysis (open coding) to reveal themes without having any pre-defined categories (Miles and Huberman, 1984), as were the teacher responses to the survey question and the secondary student responses to the three survey questions. The extraction of the codes was a manual process, carried out independently by the two authors, who then met to resolve differences.

In analysing the posters, safety- or security-related words/phrases specifically written on the posters were identified. Once minor differences had been resolved and agreement reached, each code was tallied for inclusion in the paper. Given that the majority of teacher respondents provided single word answers, there was very little opportunity for subjectivity during the analysis of teacher responses.

After the final expert focus group, the authors compared their notes and refined the visualisation accordingly, as described in Section 7.4.

4.3 Ethical Considerations

Ethical approval was obtained from the author's University's ethical review board, and permission from the head teachers of the schools, to carry out this research. The teachers were present during all activities. Before the pupils (both primary and secondary) started making their posters, they were reminded not to tell us their passwords, and also not to write their actual passwords on the posters. Ethical approval was obtained to survey the teachers and to conduct the focus groups.

5. "Cybersecurity" vs. "Cybersafety"

To inform the subsequent discussions, rigorous definitions of cybersafety and cybersecurity from the research literature are provided.

> Craigen, Diakun-Thibault, and Purse (2014, p.16) define **cybersecurity** as: "*the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights*".

This definition makes it clear that cybersecurity applies to the protection of *information* and *devices*, not necessarily the humans using such devices.

> Grey (2011, p.77) provides the following definition of **cybersafety**: "(i) the safe and responsible use of information and communication technologies (Balfour, 2005, Beach, 2007), including (ii) protection against unsolicited marketing and advertising (Frechette, 2005). Cybersafety teaches children about (iii) the positive and negative aspects of ICT

Information and Computer Security

(Livingstone, Stoilova, and Nandagiri, 2019), (iv) safeguarding against individuals who operate websites, attempt to contact children online, or to organise unsupervised meetings in person with children. Cybersafety education also involves guidance on (v) cyberethics to form a responsible attitude to the use of ICT (Berson and Berson, 2006)".

(citations embedded within definition by Grey. Roman numerals added here to facilitate discussion below).

Byron (2008) suggests that online harms can be categorised into one of the three C's: Content, Conduct and Contact. Considering the definition above, it becomes clear that harmful *Content* is captured by (ii, iii), risky *Conduct* by (i, iii, v) and harmful *Contact* by (iv).

Figure 4 compares and contrasts the key dimensions of *cybersecurity* and *cybersafety* extracted from these two definitions.

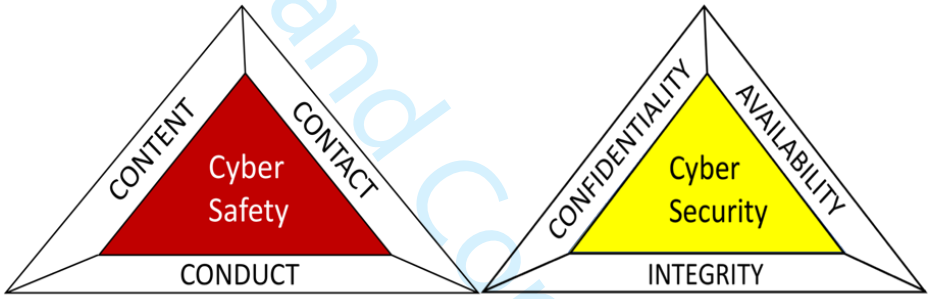

Figure 4: Cybersecurity vs. Cybersafety

It was necessary to gauge how well various stakeholders understood the nuances of, and distinctions between, the two concepts. There is already evidence that American children think that a password (a cybersecurity measure) can keep them *safe* online (Choong, Theofanos, Renaud, and Prior, 2019). Renaud and Prior (2020) also found interchangeable use of the terms in children's password-related books. Such conflation, if more widespread, might well lead online users of all ages to hold an impoverished view of the counter-measures that can be deployed to address the full range of online harms. The consequence is that children will be at risk both on and offline.

The investigation sought to determine whether this kind of conflation was more widespread. To do this: (a) a review was carried out of the usage of the terms in the academic literature (Section 5.1), (b) gauge the assurance a group of teachers thought a common cybersecurity measure (the password) afforded (Section 5.2), (c) gauge the distinctions secondary school students (aged 13-14) drew between the terms (Section 5.3), and (d) discover what 8-9 year-old children thought the purpose of a password was (Section 5.4).

Information and Computer Security

5.1 Academic Literature

An exhaustive search was carried out on the 22nd March 2020 to find publications that included "cybersecurity or cyber security" and "cybersafety or cyber safety" and "children". A hundred and forty-nine different publications were identified using Scopus and Google Scholar. Seventy-five were discarded because: (1) they were variations of other papers by the same authors, (2) they were not written in English, (3) they did not address cyber concepts, (4) they applied to systems engineering (as opposed to human understanding of concepts) or (5) they did not appear in peer-reviewed venues.

The papers from the literature search were used to gauge current usage of the two core terms. The usage by academic publication authors fell into the following categories:

Interchangeable use: Zepf (2013) reviewed a range of current cybersecurity curricula but the proposed curriculum includes a number of cybersafety aspects under this umbrella. Other publications do the same e.g. Guan and Huck (2012), Halpert (2010), Lorenz *et al.*, (2018). Marcoux (2010) examined cybersecurity websites aimed at school pupils, and also included a number of sites addressing cybersafety principles, but did not distinguish these from each other.

Naidoo *et al.*, (2013) created and evaluated a cybersafety curriculum for school children in South Africa, but it also includes cybersecurity topics such as malware and Phishing awareness. Rahman and Abindin (2019) evaluated the cybersafety awareness of primary school children in Malaysia but mention security risks in their preamble, without making a distinction between the concepts. Agarwal and Singhal (2017) also release an app to improve cybersecurity awareness but their paper title refers to Internet safety.

Von Solms and Von Solms (2014, 2015) publish papers reporting on a study into cybersafety education in South Africa, but include cybersecurity issues such as malware and hacking in their list of threats. Parris *et al.*, (2014), Kritzinger *et al.* (2017) and Van Niekerk *et al.*, (2013) do the same. Tsirtsis *et al.*, (2016) suggest a taxonomy of cybersecurity risks for minors, and include a number of cybersafety risks in their discussion e.g., online contact, cyberbullying and privacy invasion. Shillair (2016) says her paper explores cybersecurity learning under the umbrella of online safety. Vasiliev *et al.*, (2014) mention cybersecurity in the title but talks about safety in the abstract. Buscaglia and Weisman (2012) mention cybersafety in their title but refer to cybersecurity in their abstract. Razak (2016) also includes cybersafety in the title but mentions cybersecurity attacks within the paper itself. Muir (2020) does something similar in the context of home usage. Larson (2015) also includes both terms in the title of his paper but primarily focuses on cybersecurity in his discussion. Chapman (2019) consider how "safe" data is and discuss cybersecurity measures used to preserve data. Klaper and Hovy (2014), too, refer to the "safety principles" of data preservation.

Information and Computer Security

Arlitsch and Edleman (2014) make the case for people being aware of the risks to their personal and business data from cyber attacks, which crosses over to the domain of cyber privacy. Dodel and Mesch (2017) conducted a study looking at what lessons could be learnt from health behaviour models in encouraging good cyber security habits. They specifically refer to cyber safety but then mention deployment of cybersecurity measures, such as antivirus software.

Safe/Safety and Secure/Security used as a word pair: Guijar and Manhunatha (2020) use the terms "cybersafety" and "cybersecurity" but do not distinguish between them. Gurusamy and Hirani (2018) does the same. Bongiovanni (2016) considers the safety and security disruptions that could have an impact on airports in Australia. De Waal and Grosser (2008) examined how the physical aspects of "safety and security" are handled by schools. Ghazi investigate the safety and security" measures used in Egyptian hotels from the perspectives of the hotel guests. Olmstead and Smith (2017) look at the users' mistrust of institutions to protect the "safety and security" of their personal data.

Applying safety techniques to cybersecurity: Paul and Rioux (2015) provide a literature review of papers which investigate both safety and security architecting as well as papers which investigate engineering specialities. Salim and Madnick (2016) argue for cybersecurity risks to be managed in the same way as systems' safety.

Using cybersecurity measures to ensure cybersafety: Tsirtsis *et al.* (2016) talk about using Internet filtering, data analytics, advanced content analysis and data mining to protect children online. Nandhini and Moorthi (2018) and Gao, Guo, Xie, Luo, Lu, and Yan (2017) review the viability of wearable smart devices in enhancing safety. Tsai, Jiang, Alhabash, LaRose, Rifon, and Cotton (2016) consider whether protection motivation theory predicts the use of preventative cyber measures. Bloomfield, Netkachova, and Stroud (2013) argue that devices can only assure cybersafety if they are properly secured.

Cybersafety only: A range of publications deal with cyber bullying, digital citizenship and cyber safety education (Heider and Jalongo , 2015; Crescenzi-Lanna, Valente, and Suárez-Gómez, 2019; Roberto, Eden, Savage, Ramos-Salazar, and Deiss, 2014; Englander, 2017; Mishna, Saini, and Solomon, 2009; Milosevic and Livingstone, 2017; Paunović, 2018; Grey, 2011; Edwards, Nolan, Henderson, Skouteris, Mantilla, Lambert, and Bird, 2016b; Hanewald, 2008; Jadambaa, Thomas, Scott, Graves, Brain, and Pacella, 2019; Martin and Rice, 2012; Tsatsanashvili, 2018; Mutula, 2008; Ahmad, Arifin, Asma'Mokhtar, Hood, Tiun, and Jambari, 2019; Dooley *et al.*, 2009).

Information and Computer Security

Cybersecurity only: Lastdrager, Gallardo, Hartel, and Junger (2017) talk about training children to spot Phishing messages. , Brittan, Jahankhani, and McCarthy (2018) are concerned about raising cyber security awareness in children. Dlamini *et al.*, (2011) reviewed African countries' cyber security policies. Giannakas, Kambourakis, Papasalouros, and Gritzalis (2016) discuss the development of an app called CyberAware to improve cybersecurity awareness.

Cybersafety and cybersecurity used as distinct terms: Butler (2010) makes a distinction between cybersecurity (e.g., avoiding viruses) and cybersafety teaching (how to avoid online predators; cyberethics, appropriate and respectful online behaviour and the consequences of cyberbullying). Chen and Shen (2016) provide definitions. Cybersafety is defined as: "*the ability to act in a safe and responsible manner on the Internet and other connected environments*" (p. 2), while they explain that cybsersecurity "*covers physical protection (both hardware and software) of personal information and technology resources from unauthorized access gained via technological means*" (p. 2). Pusey and Sadera (2011) define cybersafety as: "*the actions individuals take to minimize the dangers they could encounter when using Internet-capable technology*" (p. 82). They explain that cybersecurity "*includes antivirus software, Internet content filters, firewalls, and password protection*" (p. 82). Tonge, Kasture, and Chaudhari (2013) agree that cybersafety is related to the *social* aspects of Internet usage, while cybersecurity is related to the protection of resources. DeFranco (2011) also makes these distinctions between the terms.

Summary: This investigation revealed a great deal of interchangeable use of the core terms, and their use in non-reversible word pairs, which indicates that authors are not making a clear distinction between the terms in many cases. Only a handful make clear distinctions between the terms, as outlined in the previous paragraph.

5.2. Teachers

5.2.1 Methodology

To assess whether teachers had a clear idea of the distinctions between the terms, they could have been asked to define the terms, but this would not necessarily have been effective. Given that children in Scotland (where this research was carried out) are given a password within a week or two of starting school, and that teachers manage their use thereof, it was decided to focus on what the respondents thought this commonly-used cybersecurity measure could deliver and what its purpose is. Cybersafety-focused responses would suggest that participants did not make a distinction between concepts.

Information and Computer Security

Teachers were asked: "*In your opinion, the purposes of a password for children are:*". Three open-text entry fields elicited responses.

This question was published in an online survey using Qualtrics and then advertised on teacher-specific fora, via emails sent to schools by contacts in the national educational authority and by personal contacts with primary school teachers.

5.2.2 Findings

Ninety-five responses were received. After removing incomplete and nonsense responses, 56 responses remained to support analysis, with 146 distinct answers to the question. The authors coded the responses independently then met to agree on codes. Table 1 shows the codes that appeared more than once in the responses.

Table 1: Codes for Password Reasons Provided by Respondents

Code	**#**	**Code**	**#**
Safety	31	Responsibility	7
Password education	25	Prove Identity	2
Access control	22	Personalisation	7
Security	20	Age Verification	4
Protection	17	Password Issues	8

5.2.3 Discussion

The only absolutely correct answers are "*access control*" and "*prove identity*" (16% of the responses), with "security" being an acceptable approximation of the umbrella nature of security (all three making up 30% of the responses). The use of passwords to facilitate education is an understandable response, given that these were all primary school teachers. However, the posed question did not include the word "in school": it is a more general question which ought to have elicited cybersecurity-related justifications. The predominant use of "safety" suggests that teachers are conflating concepts. A password, by itself, cannot keep a child *safe* in the online world.

5.3. Secondary School Pupils

5.3.1 Methodology

An outreach event for 13-14 year old secondary school pupils was hosted at the authors' institution. Groups of students created posters about what people should know about passwords. Eleven of these

Information and Computer Security

were collected. Given that these secondary school pupils could express their understanding of concepts in words, and to have learnt the distinctions between the concepts, they were also asked to complete an online survey with the following questions:

1) Can a strong password keep you safe online?
2) Can a strong password keep your online account secure?
3) What do you think the difference is between "cyber safety" and "cyber security"?

The students were then given a lesson on password good practice.

5.3.2 Findings

On the posters, two groups mentioned secure/security (once on each poster) and one mentioned safety. Thirty six of fifty students responded to the survey, anonymously.

1. Can a strong password keep you safe online? Thirty-three pupils thought a password could keep them safe online, one was unsure, while two said it could not. This shows that the majority of these pupils were erroneously putting their faith in a cybersecurity mechanism to preserve their cybersafety.

2. Can a strong password keep your online account secure? Twenty-six pupils correctly judged that a password could keep accounts secure, four were unsure, while six said it could not. The majority did indeed answer correctly.

3. What do you think the difference is between "cyber safety" and "cyber security"? Twelve (a third) of the students said they did not know the difference. Of the rest, many demonstrated conflation. For example:

- "*Cyber safety is to do with phishing etc, and cyber security is to do with passwords etc.*".
- "*Cyber safety is to do with cyber attacks, cyber security is how secure your accounts are e.g., passwords*".
- "*One is to prevent you from doing something wrong and the other is to prevent hackers from getting your information*".
- "*Cyber safety is to do with phishing etc, and cyber security is to do with passwords etc.*"

Information and Computer Security

5.3.3 Discussion

Only one survey response came close to correctly distinguishing the concepts: "*Safety is when we are considering our personal safety and security is the safety of personal details*".

This survey confirmed that children do not learn to distinguish between the core terms as they go through the educational system. It is concerning that the surveyed secondary pupils are in the "*most at risk*" online age group (Fleming, Greentree, Cocotti-Muller, Elias, & Morrison, 2006), but do not seem to understand the differences between their own cybersafety and the affordances of cybersecurity counter-measures.

5.4. Primary School Pupils

5.4.1 Methodology

Four primary schools were visited. A lesson on password good practice was delivered to five classes of 8-9 year old children (2 at one school and 1 each at the other four schools). To ensure that responses were not primed, and that discussions were not framed, the class commenced by asking them to create a poster (individually) to say what people ought to know about passwords (A3 sheets, stickers and coloured felt tipped pens were provided). The ethical review board required the session to commence with an admonition that the children not share passwords with anyone (before they started making the posters), but this was the only framing they received. A hundred and forty-one individually produced anonymous posters were collected. Afterwards, a lesson on password good practice was delivered.

5.4.2 Findings

The use of the words "secure", "security", "safe" or "safety" was monitored on the posters. Four posters mentioned secure/security, and 21 posters mentioned safety. Of those that mentioned safe/safety, several mentioned it more than once: Forty-three blocks of information mention safety/safe. The following quotes emerged, in two categories.

Personal, Password or Ambiguous Safety: "*Get password safe*"; "*Keep your password safe*"; "*Unsafe and Safe Passwords*"; "*Be safe on the internet*"; "*You need to stay safe*"; "*Safe/What good things you should know*"; "*You need a safe password*"; "*Keep them safe*"; "*What is a password: Keep us safe*"; "*Keep your passwords safe*"; "*Always keep your passwords safe*"; "*Better safe than sorry*".

Information and Computer Security

Device Safety: "*Passwords are something that keep a phone or iPad safe it can also keep a laptop safe*" and "*If you have a password, your device will be secure. Do not tell anyone your password or your device won't be safe*".

5.4.1 Discussion

These posters confirmed that there was much interchangeable use of the safety and security terms, as first reported by Choong et al. (2019). Bear in mind that the children were asked to make posters about "password good practice". They had perhaps heard adults use these two core terms interchangeably, and their usage reflected this.

5.5. Summary & Implications

This review demonstrates concept conflation and interchangeable usage across the board, confirming Choong *et al.*'s (2019) findings. The reality is that 'cybersecurity' and 'cybersafety' concepts are related and interdependent but, crucially, require different combinations of actions to manage and ameliorate them.

Due to concept conflation, the participants appeared to put their faith in cybersecurity tools to keep children cybersafe. While strong passwords contribute to cybersafety they do not, in and of themselves, guarantee cybersafety. Consider Terry, a child who has a social networking account. Terry's parents ensure that a strong password is used and think this will keep her safe. Terry befriends children from her school. One day, a friend request arrives from someone Terry does not recognise, but Terry is reassured by the childlike appearance of the profile photo. She accepts the friend request and is now at risk. The new "friend" is actually an online groomer. This groomer might post inappropriate content, which he invites Terry to view. Having a strong password has not kept Terry safe. Terry's information is indeed protected by a strong secret password, but her physical safety might still be at risk, so teachers and carers might not even be aware of this. To ensure that adult stakeholders understand the nuances, the required details to facilitate the development of the knowledge transfer mechanism are derived in the next Section.

6. Scoping the Core Concepts

It is important for those with caring responsibilities to understand the differences, because children are particularly vulnerable as they navigate the online world (Livingstone *et al.*, 2014). Their carers and educators, if they understand what to do, can help protect their charges from online harms by deploying counter-measures.

Information and Computer Security

To support creation of a rigorously grounded resource pack, the following are required:

6.1 — *Risky Behaviours*: A comprehensive list of risky online behaviours from the research literature, as well as child charity and government publications (Section 6.1).
6.2 — *Ages*: that the children are likely to engage in each of the behaviours, because this is a differentiating factor in online experiences (Livingstone, Davidson and Bryce, 2017) (Section 6.2).
6.3 — *Counter-Measures*: to empower adult stakeholders to manage risks and prevent harms (United Nations, 2015) (Section 6.3).
6.4 – *Validation* of these lists (Section 6.4).

6.1. Risky Online Behaviours

To compile a list of risky behaviours, the papers gathered during Phase 1 were perused to search for risky behaviours. Then, other child-related publications were used to confirm these and to ensure comprehensiveness. The initial list of child-related risky behaviours that emerged from this stage is provided in Table 2.

Table 2. Examples of harmful online actions from the literature

6.1.1 Focus Groups

Focus groups were conducted to validate the comprehensiveness of the behaviour list. Trainee and qualified teachers were recruited, as well as a higher education lecturer and a retired teacher, to participate in focus groups. Six virtual focus groups were conducted, with 1, 3, 1, 2, 2, and 2 participants (some participants did not connect so sometimes only one participant participated). The topics of cybersafety & cybersecurity were introduced, as were child-related online behaviours and potential harms. They were then shown the list of risky behaviours that had been identified, one at a time, and asked to consider whether any risky behaviours and potential harms had been omitted. Table 3 presents the additional risky behaviours that emerged from this set of focus groups.

Table 3: New Risky Behaviours that Emerged from the Focus Groups

6.2. Ages

The academic and grey literature were consulted to determine the ages at which children are most likely to engage in different risky behaviours (Table 4)

Table 4: Ages at which children are likely to engage in specific risky behaviours

Information and Computer Security

6.3. Counter-Measures

Byron (2008) suggests three broad categories of measures: reduce availability (industry and government responsibility), reduce access (industry and carers) and increase resilience (parents talking to their children, by following advice that is offered by various bodies).

Aynsley (2014) suggests a four-part framework of online harm management measures: the PIES model, which includes policies and practices; infrastructure; education; and standards. This model has been particularly useful in schools, especially in terms of formulating acceptable use policies (Becta, 2009).

The aim of this research is to focus primarily on the measures that can be employed by teachers and carers, within the home or school. Online sources provide helpful strategies for keeping children safe online, as shown in Table 6. These fall naturally into three categories, making up the three M's:

Mentor (Byron's increased resilience): a range of activities that carers undertake to help their children to navigate the online world in a responsible way. (internetmatters.org, 2018; Childnet International, 2018; UK Council for Internet Safety, 2020a; UK Council for Internet Safety, 2016; eSafetyCommissioner, 2020; ThinkUKnow, undated-a)

Mitigate (Byron's reduction of access): the deployment of technological solutions or configurations to reduce the threat leading to the harm (internetmatters.org, 2018; Childnet International, 2018; UK Council for Internet Safety, 2020a; UK Council for Internet Safety, 2016; eSafetyCommissioner, 2020; ThinkUKnow, undated-a)

Monitor (chaperoning activities): the deployment of technology to monitor the child's activities either in real time or retrospectively. This is to allow the parent to tailor mentoring activities when mentoring and mitigation efforts have been insufficient. (internetmatters.org, 2018; UK Council for Internet Safety, 2016; eSafetyCommissioner, 2020; ThinkUKnow, undated-a)

The full list of behaviour-harm pairs could now be mapped to risk management counter-measures, as shown in Table 5. A literature search (both academic and grey literature) was used to identify counter-measures. Each was categorised as one of the three M's: *mentor, mitigate* or *monitor*.

Table 5. Mapping Harms to Measures

Information and Computer Security

6.4. Webinar

The final mapping of harms to counter measures was presented during a Webinar, where 98 Nigerian participants agreed to evaluate the comprehensiveness and correctness of the list of harms and counter measures. An introduction to child-related harms was provided, and then each of the risky behaviours and harms was prevented, while the presenter spoke about how they could be managed, and harms prevented. After the webinar, an email containing a link to an online Google form was sent to participants. They could use this to comment anonymously. The form presented the behaviours one at a time to allow feedback, and then concluded by asking them to name any that had been left out.

Thirteen participants provided feedback. The responses confirmed the comprehensiveness of the list of harms and their counter-measures. For example, to mitigate against viruses: "*Use of current anti-virus, stop downloading free applications whose sources are unknown, always check that external units are virus free before connecting and downloading information from them*." For phishing, an example response was: "*Educating about suspicious online messages*." In terms of discouraging children from engaging in hacking activities, one respondent said: "*Educate them on the dangers they expose themselves and their families to by so doing*."

In terms of the comprehensiveness of the behaviour list, two comments are noteworthy: (1) "*Child labor, (making children do jobs online like driving traffic to a particular site, or sharing advertising messages, or campaign messages)*" and (2) "*There are instances whereby parents carelessly leave their devices and children get access to adult content on them, even though the devices are not connected to the Internet*". While these are valid harms, they do not really fit because the resource is intended to help adult stakeholders to implement counter-measures. The underlying assumption is that such adults are responsible and careful. The counter-measures required to address these two harms will be different from those presented here and are thus not included in the visualisation.

7. Developing the Resource Pack

There are four inter-related dimensions to be communicated to adult stakeholders: (a) risky behaviours, (b) harms, (c) countermeasures, and (d) vulnerable age ranges. This would be challenging to communicate understandably in a textual format. Visualising knowledge, on the other hand, benefits from the power of human visual processing capabilities and makes such communication more effective and efficient in transferring the knowledge. Renaud and Van Biljon (2019) explain that visualisations have superior "communicative power". Hence, a visualisation was chosen to communicate the domain knowledge to adult stakeholders.

Information and Computer Security

Teachers were targeted as an audience for the resource in the first instance, because of their crucial role in protecting children from online risks (Dönmez, Odabaşı, Yurdakul, Kuzu, and Girgin, 2017; Shin and Lwin, 2017; Livingstone and Bober, 2004). Posters are a widely used form of visualisation, intended to be displayed to ensure exposure to the knowledge in a variety of contexts e.g., COVID (Chen, 2020), health promotion (Ward and Hawthorne, 1994), adverse weather events (Parker, 1999) and, crucially, in education (Duchin and Sherwood, 1990). This research suggested that a poster would be a feasible mechanism for conveying this knowledge to teachers, and then to provide a similarly tailored resource to parents as future work.

The resource to convey the knowledge would thus consist of:

(1) a visualisation to provide an overview, and

(2) accompanying information to provide more detail.

Providing these two co-dependent resources embraces Shneiderman's principle of "*overview and detail-on-demand*" (Shneiderman, 1996).

7.1 Crafting the Visualisation

Renaud and Van Biljon (2019) suggest that when knowledge is to be transferred by a visualisation, four questions should be answered:

(1) ***Why*** *visualise?* Section 4 showed that there is confusion, at the moment, about the kinds of counter measures that should be deployed. There is evidence that visual knowledge transfer mechanisms are more powerful than text (Du, 2018).

(2) ***For whom*** *is it being visualised?* There is evidence that adult stakeholders need more resources to help them to understand the nuances and dimensions of the cybersecurity and cybersafety space (see Section 5).

(3) ***What*** *knowledge is to be visualised?* The visualisation should communicate the following intersecting concepts:

   a. *Risky Behaviour and Potential Harms* - a short descriptor and an example of a potential resulting harm to elucidate (Table 3).
   b. *Age Groups* - mapping the risky behaviours to the ages at which children are likely to be tempted to engage in them (Table 4).
   c. *Counter-Measures* - mapping harms to one or more of the three Ms' counter-measure categories (Table 5).

Information and Computer Security

(4) ***How*** *should it be visualised?* Renaud and Van Biljon (2019) advise maximising clarity, consistency and simplicity. They also suggest including text in the visualisation to enhance clarity and pay attention to aesthetics.

7.2 Expert Focus Group

An initial draft visualisation was produced. Ten cyber security academics, a CISO, and two Secondary School teachers critiqued it in terms of understandability, comprehensiveness and simplicity. The content was subsequently revised as follows:

1) *Remove Phishing*. This topic was considered too complex to include because many adults are not able to identify Phishing messages and children might also struggle with this. Moreover, Phish detection requires capability building, not awareness raising *per se*.
2) *Simplify the visualisation* by collapsing the categories that require the same actions to be taken. As a consequence, the 4-8 year age group would only have three categories of risky behaviours.
    a. Sharing Passwords (H5)
    b. Unconfigured Smart Devices (H17, H14, H4)
    c. Consuming harmful content/advertising (H2, H11, H3).
3) *Expand categories* where the consequences might be different. This applied specifically to 10+ category, where the following risky behaviours ought to be specifically highlighted:
    a. H9: Revenge Porn – which is illegal, and could lead to law enforcement becoming involved.
    b. Splitting H2: Adding the consumption of content that normalises harmful behaviours e.g. self harming and radicalisation.

The final visualisation was drawn by a graphical designer to ensure that it maximised aesthetics, clarity and consistency, as advised by Renaud and Van Biljon (2019) (Figure 5).

7.3 Accompanying Information

Three main categories of countermeasures will be expanded upon:

Mentor:
Children should be taught password "good practice" principles (H5) (Prior and Renaud, 2020), and also be made aware of their part in mitigating particular harms (H4). For example, that they should disclose as little personal information as possible online (H1), that they should not believe everything

Information and Computer Security

they see online (H3), and that there are bad actors online who might pretend to be children (H10) or want to sell them things (H11).

Education, on its own, is never going to be sufficient unless the child is able to discuss matters with a trusted adult — their carer or teacher. This is crucial, especially in cases where a groomer is making initial attempts to stalk the child (H10), or in cases where the child has perhaps behaved unwisely online and needs assistance to correct the situation (H9,H16) or to cope with the impact on their psyche (H2).

Mitigate:

This includes ensuring due diligence efforts including: (1) ensuring that the WiFi password is strong (H14, H17), (2) that default passwords on all home and child smart devices are changed (H14), (3) set the browser's home page to a child friendly site (internetmatters.org, 2018), (4) Use child friendly search engines (e.g. Swiggle, Kids Search), and safe browser settings[2] (H2) (internetmatters.org, 2018), (5) Safe search settings can be activated on Google, YouTube, iTunes and iPlayer (H2) (internetmatters.org, 2018), and (6) if a child is using a new site, check it out, and check age ratings (H16). For example, Facebook and Instagram require children to be 13. Carers should enforce this. (7) install advert blockers (H10) (Cook, 2019),

It also includes the installation of software to mitigate some of the harms (UK Council for Internet Safety, 2020b) (e.g.): (1) if a child is likely to connect to a public WiFi, the carer should install a VPN on the child's device (H12) (Child Safe VPN, 2020), (2) install anti-virus, anti-malware and anti-phish software (H7).

If connecting to a Public WiFi, look out for friendly WiFi symbols like Mumsnet Family Friendly WiFi (H12) (internetmatters.org, 2018).

Monitor:

A range of tools are available, including web filtering software and parental controls (H2, H3, H11) (Geier, 2013), and behaviour monitoring software e.g. Mozilla parent control add on[3] or Google StopItKids add on[4] (H6) (Price, 2020).

The resource pack is available from https://cybersquad.uk/resources.html

[2] https://www.searchrpm.com/internet-safety-for-kids/parent-resources/safe-browser-settings-for-kids
[3] https://addons.mozilla.org/en-US/firefox/addon/family-friendly-filter/
[4] https://chrome.google.com/webstore/detail/stopitkids-parental-contr/ogbomkfadhhndgccgfknejchfhkcolko

Information and Computer Security

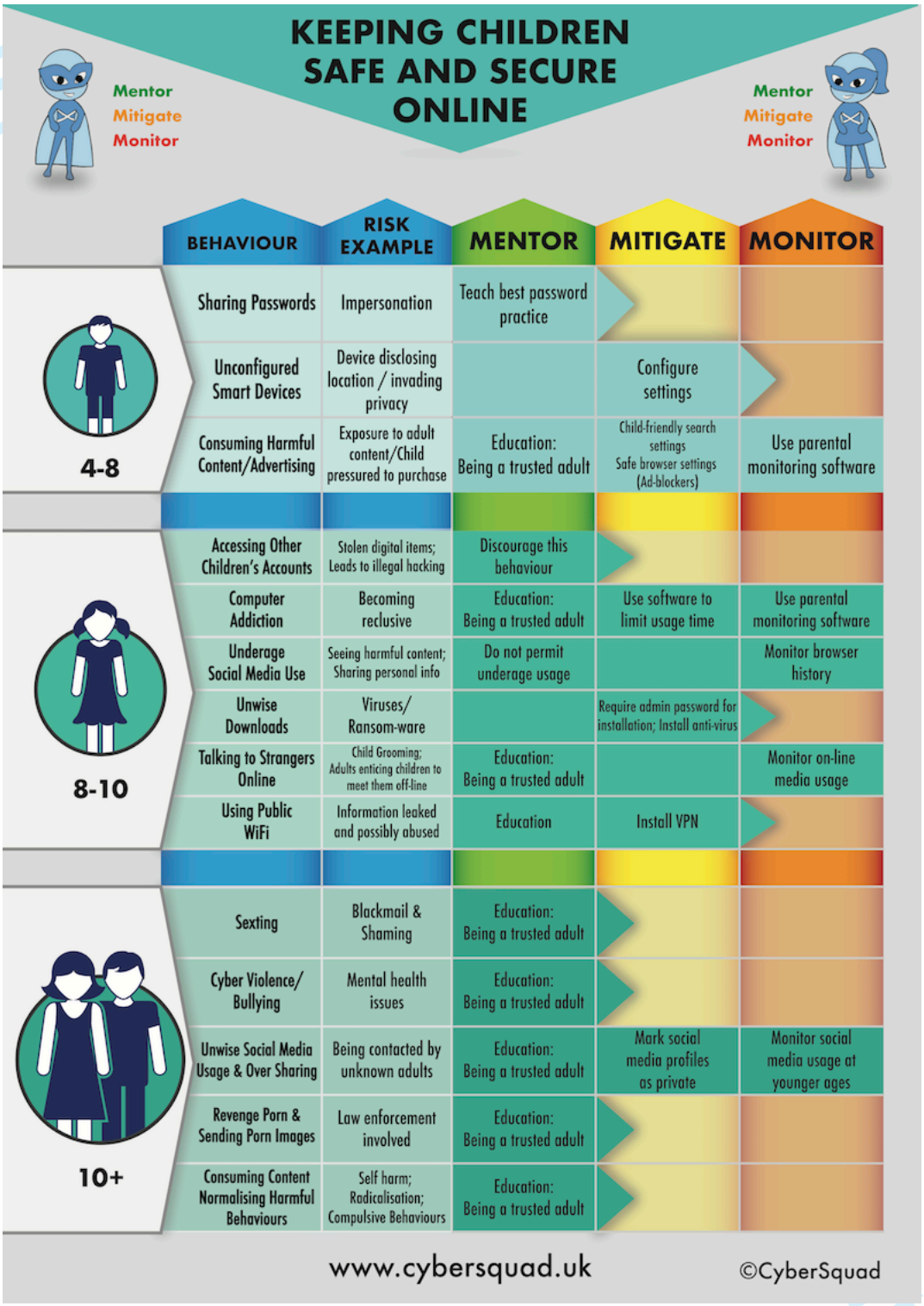

Figure 5. Final Visualisation

8. Discussion & Reflection

The research question was:

> ***"How best** can adult stakeholders be helped to **understand** the **full range of risky online behaviours** and the **appropriate countermeasures** that they can take to prevent online harms to the children in their care?"*

Section 5 confirms the need for an intervention to enhance understanding.

(1) To ensure ***a full range of risky online behaviours and appropriate countermeasures,*** Section 6 reports on the research conducted to ensure that the four dimensions of the online harm space were comprehensively scoped in Section 6.

(2) ***How best*** to communicate the information? A visualisation in poster format was proposed, instead of pure text, and motivated in Section 7.

(3) To enhance ***understanding*** the visualisation was crafted (Section 7.1), and then validated by experts during a focus group (Section 7.2).

An educational resource pack was developed to enhance awareness and improve comprehension of both cybersecurity and cybersafety domains. This resource contains a poster visualising the knowledge, together with an information pack to expand on the overview provided by the poster.

8.1. Limitations

The visualisation does not include cyberprivacy examples. The decision was made to omit this during the initial visualisation refinement. Essentially, it was realised that the visualisation needed to be simple and clear enough to eliminate the confusion that had been evidenced. As a next step, it would be necessary to extend this visualisation with more concepts, so as to provide caregivers with a step-by-step progression of visualisations to engender a more nuanced understanding of all the cyber-related terms.

Another limitation is that the number of survey participants is relatively small. This is generally acceptable for studies with a strong qualitative component, such as this one, where it is important to reveal mental models (Mason, 2010).

Information and Computer Security

9. Conclusion & Future Work

The research reported in this paper was undertaken to find out how best to help adult stakeholders to understand the full range of online risky behaviours and the countermeasures that they can take to prevent online harms to the children in their care. A number of studies were carried out to determine how well people understood the domain. Widespread conflation of the two core terms of "cybersecurity" and "cybersafety" was revealed, confirming the need to communicate all the dimensions of this field more effectively. A list of online risky behaviours, online harms and counter measures was compiled, and the ages at which children were likely to start engaging in these risky behaviours determined. Because it was necessary to communicate four dimensions, a visualisation was considered to be the best way of doing this. This research engaged with a variety of stakeholders throughout the process, to ensure that the final visualisation would be as comprehensive and helpful as possible. The final resource pack, containing the visualisation together with an information sheet, should help adult stakeholders to understand the nuances of the online harm domain, and become aware of the counter measures they can use to protect the children in their care. The content and appearance of the pack was grounded in the research literature and also benefited from the inputs of domain experts in refining it. This resource pack is provided to assist all adults with children in their care.

There is a need to support adult stakeholders more effectively in protecting their children in the online domain. A longer-term intervention would integrate this resource pack into teacher training curricula or provide information sessions for parents. We hope that the visualisation proposed here will serve as an interim measure, a way of delivering crucial information directly to teachers, in an accessible and easy-to-process format. It also serves to open a discourse with all adult stakeholders, which will help us to develop further resources to support and inform them. In particular, the next research stage will target parents to ensure that knowledge is transferred to them too, given that the initial pack was targeted at teachers in the school context.

Acknowledgements

The authors are grateful to the teachers and pupils who invited us into their classrooms and to those who responded to the surveys. It has been a tremendous privilege interacting with educators and children and doing this research. We also thank the focus group and webinar participants, without whom this research would not have been possible. We thank Ivano Bongiovanni for giving us feedback and helping us to improve the final visualisation and Ethan Bayne and Ross Heenan for helping us to understand the range of technical measures that can be deployed as counter-measures. We also thank the expert reviewers, and the authors' colleagues at Abertay University. We thank Keagan Renaud for

Information and Computer Security

producing the final visualisation. Last, but not least, we thank our anonymous reviewers for their helpful feedback.

References

Agarwal, A. & Singhal, A. (2017). Securing Our Digital Natives: a Study of Commonly Experience Internet Safety Issues and a One-Stop Solution. In *Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance*, pages 178–186, New Delhi, India.

Ahmad, N., Arifin, A., Asma'Mokhtar, U., Hood, Z., Tiun, A. & Jambari, D. I. (2019). Parental awareness on cyber threats using social media. *Jurnal Komunikasi: Malaysian Journal of Communication*, 35(2). https://ejournal.ukm.my/mjc/article/view/33515/0.

Ahmed, T., Shaffer, P., Connelly, K., Crandall, D. & Kapadia A. (2016). Addressing physical safety, security, and privacy for people with visual impairments. In *Twelfth Symposium on Usable Privacy and Security (SOUPS)*, (pp. 341–354).

Alotaibi, F., Furnell, S., Stengel, I. & Papadaki, M. (2016). A review of using gaming technology for cyber-security awareness. *Int. J. Inf. Secur. Res.(IJISR)*, 6(2), 660–666. https://doi.org/10.20533/ijisr.2042.4639.2016.0076.

Al Shamsi, A.A. (2019). Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE. *International Journal of Information Technology and Language Studies*, 3 (2), 8-29.

Annansingh, F., & Veli, T. (2016). An investigation into risks awareness and e-safety needs of children on the internet. *Interactive Technology and Smart Education*. 13 (2) 147-165. https://doi.org/10.1108/ITSE-09-2015-0029

Arlitsch, K. & Edelman, A. (2014). Staying safe: Cyber security for people and organizations. *Journal of Library Administration*, 54(1), 46–56. https://doi.org/10.1080/01930826.2014.893116.

Attached Mama. (2009). *7 ways to prevent cyberbullying*. Retreived 27 May 2020, from http://www.ecobabysteps.com/2009/11/27/what-is-a-parent-to-do-about-children-and-consumerism/

Aynsley, C. (2014). *Keeping children safe online a guide for organisations*. Retrieved 31 May 2020, from www.keepingchildrensafe.org.uk.

Balfour, C. (2005). A journey of social change: Turning government digital strategy into cybersafe local school practice, 2005. Paper presented at the *Safety & Security in a Networked World: Balancing Cyber-rights & Responsibilities conference*, Oxford, UK.

Barbara, N. (2020). *Best antivirus software options: Why to use an antivirus?* Retrieved 27 May 2020, from https://worthgram.com/best-antivirus-software-options/

Beach, R. (2007). New Zealand's first steps to cybersafety. *Paper presented at the Early Childhood Convention*, Rotorua, NZ.

Becta. (2009). *AUPs in context: Establishing safe and responsible online behaviours*. Retrieved 31 May 2020, from www.becta. org.uk

Bednarowska, Z. (2015). Desk research — exploiting the potential of secondary data in market and social research. *Marketing i Rynek*, 7(2015), 18-26.

Ben-Joseph, E. P. (2018). *Internet Safety* (KidsHealth). Retrieved 17 December from: https://kidshealth.org/en/parents/net-safety.html

Berson, I. R., and Berson, M. J. (2006). Children and Their Digital Dossiers: Lessons in Privacy Rights in the Digital Age. *International Journal of Social Education*, 21(1), 135–147.

Berson, M. J., & Berson, I. R. (2003). Lessons learned about schools and their responsibility to foster safety online. *Journal of School Violence*, 2(1), 105-117.

Bloomfield, R., Netkachova, K. & Stroud, R. (2013). Security-informed safety: if it's not secure, it's not safe. In *International Workshop on Software Engineering for Resilient Systems*, (pp. 17–32.) Springer.

Information and Computer Security

Bongiovanni, I. (2016). *Assessing Vulnerability to Safety and Security Disruptions in Australian Airports*. PhD thesis, Queensland University of Technology – QUT.

Boyd, B., Marwick, A., Aftab, P. & Koeltl, M. (2009). Conundrum of visibility. *Children and Media*, 3(4), 410–419. https://doi.org/10.1080/17482790903233465.

Brittan, T., Jahankhani, H., & McCarthy, J. (2018). An examination into the effect of early education on cyber security awareness within the UK. In *Cyber Criminology*, (pp. 291–306). Springer.

Buscaglia, C. A. & Weismann, M. F. (2012). How "Cybersafe" Are the BRICs? *Journal of Legal, Ethical and Regulatory Issues*, 15(2), 61–65.

Butler, K. (2010). Cybersafety in the classroom: district leaders need to take responsibility for teaching students how to wisely navigate the Internet. *District Administration*, 46(6), 53-54,56-57.

Byron, T. (2008). *Safer children in a digital world the report of the Byron review*. Retrieved 31 May 2020, from https://childcentre.info

Chappell Jr, R.P. (2012). *Child identity theft: What every parent needs to know*. Rowman & Littlefield Publishers.

Chen, I. L. & Shen, L. (2016). The cyberethics, cybersafety, and cybersecurity at schools. *International Journal of Cyber Ethics in Education (IJCEE)*, 4(1), 1–15. https://doi.org/10.4018/IJCEE.2016010101.

Chen, N. (2020). Semiotic Resourcefulness in Crisis Risk Communication: The Case of COVID-19 Posters. *Language and Semiotic Studies* 6(3). http://lass.suda.edu.cn/39/7b/c13719a407931/page.htm

Chapman, J. (2019). How safe is your data? Cyber-security in higher education. *Higher Education Policy Institute Policy*. Retrieved June 2020, from https://www.hepi.ac.uk/wp-content/uploads/2019/03/Policy-Note-12-Paper-April-2019-How-safe-is-your-data.pdf

Child Rights International Network (CRIN). (2019) Response of the Child Rights International Network (CRIN) to the Open Consultation on the Online Harms White Paper. Retrieved 17 December 2020 from https://home.crin.org/issues/digital-rights/online-harms

Childnet International. (2018). *Parents and carers*. Retrieved 31 May 2020, from https://www.childnet.com/parents-and-carers

Child Safe VPN. (2020). *Welcome to child safe VPN*. Retrieved 2 June 2020, from https://childsafevpn.com

Choi, C. (2018). *New rules to prevent children's 'smart' toys from being hacked*. Pen Test Partners. Retrieved 27 May 2020, from https://www.itv.com/news/2018-11-21/new-rules-on-internet-toy-security/

Choong, Y-Y., Theofanos, M., Renaud, K. & Prior, A. (2019). Case study – exploring children's password knowledge and practices. In *Usable Security (USEC)*, San Diego, USA. https://www.ndss-symposium.org/wp-content/uploads/2019/02/usec2019_04-5_Choong_paper.pdf

Christensen, L and Aldridge, J. (2012). *Critical pedagogy for early childhood and elementary educators*. Springer Science & Business Media, New York and London.

Clarke, C. (2002). The internet according to kids. *Young Consumers: Insight and Ideas for Responsible Marketers*, 3(2), 45–52.

common sense media. (undated). *Privacy and internet safety*. Retrieved 2 June 2020, from https://www.commonsensemedia. org/privacy-and-internet-safety/how-do-i-protect-my-kids-privacy-online

Conroy, S. (2007). *Labor's plan for cyber-safety*, Retrieved 29 December 2019, from https://www.cla.asn.au/Articles/labors_plan_for_cyber_safety.pdf

Comartin, E., Kernsmith, R. and Kernsmith, P. (2013) "Sexting" and Sex Offender Registration: Do Age, Gender, and Sexual Orientation Matter?, *Deviant Behavior*, 34:1, 38-52, DOI: 10.1080/01639625.2012.707534

Cook, S. (2019). *10 best free ad blockers to remove ads and popups*. Retrieved 27 May 2020, from https://www.comparitech.com/blog/vpn-privacy/best-free-ad-blockers/

Craigen, D., Diakun-Thibault, N. & Purse, R. (2014). Defining cyber-security. *Technology Innovation Management Review*, 4(10), 13–21. http://doi.org/10.22215/timreview/835.

Information and computer security

Crescenzi-Lanna, L., Valente, R. and Rafael Suárez-Gómez. (2019). Safe and inclusive educational apps: *Digital protection from an ethical and critical perspective. Comunicar*, 27(61), 93–102. https://doi.org/10.3916/C61-2019-08.

Creswell, J. W. (1999). Mixed-method research: Introduction and application. In *Handbook of educational policy* (pp. 455-472). Academic Press.

Crotty, M. (1998). The foundations of social research: Meaning and perspective in the research process. Sage, London UK.

Davidson, J., Grove-Hills, J., Bifulco, A., Gottschalk, P., Caretti, V., Pham, T. and Webster, S. (2011) Online abuse: Literature review and policy context. Project Report) *European Online Grooming Project*. Retrieved January 2021 from: http://childcentre.info/robert/extensions/robert/doc/99f4c1bbb0876c9838d493b8c406a121.pdf

Davis, A. C., Wright, C., Curtis, M., Hellard, M. E., Lim, M. S. C., & Temple-Smith, M. J. (2019). 'Not my child': parenting, pornography, and views on education. *Journal of Family Studies*, 1-16.

DeFranco, J. F. (2011). Teaching Internet Security, Safety in Our Classrooms. *Techniques: Connecting Education and Careers* (*J1*), 86(5), 52–55.

De Waal, E. & Grösser, M. M. (2009). Safety and security at school: A pedagogical perspective. *Teaching and Teacher Education*, 25(5), 697–706. https://doi.org/10.1016/j.tate.2008.12.002.

Dlamini, I.Z., Taute,B. & Radebe, J. (2011). Framework for an African policy towards creating cyber security awareness. In *Proceedings of Southern African Cyber Security Awareness Workshop (SACSAW),* (pp. 15–31).

Dlamini, Z. & Modise, M. (2013). Cyber security awareness initiatives in South Africa: a synergy approach. *Case Study. Inf. Warf. Secur. Res. Teach. Stud*, (pp. 1-22).

Dodel, M. & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior*, 68, 359–367. https://doi.org/10. 1016/j.chb.2016.11.044.

Dönmez, O., Odabaşı, H. F., Yurdakul, I. K., Kuzu, A., & Girgin, Ü. (2017). Development of a scale to address perceptions of pre-service teachers regarding online risks for children. *Educational Sciences: Theory & Practice*, *17*(3), 923-943.

Dooley, J. J., Cross, D., Hearn, L., & Treyvaud, R. (2009). Review of existing Australian and international cyber-safety research. Technical report, *Child Health Promotion Research Centre*, Edith Cowan University, 2009. Retrieved January 2021 from: https://ro.ecu.edu.au/ecuworks/7223/

Döring, N. (2014). Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting? *Cyberpsychology*: *Journal of Psychosocial Research on Cyberspace*, 8(1). Article 9. https://doi.org/10.5817/CP2014-1-9

Du, H. (2018). The employment of knowledge visualisation to facilitate tacit knowledge sharing (Doctoral dissertation, Management Systems, The University of Waikato).

Duchin, S., & Sherwood, G. (1990). Posters as an educational strategy. *The Journal of Continuing Education in Nursing*, *21*(5), 205-208.

Edwards, S., Nolan, A., Henderson, M., Skouteris, H., Mantilla, A., Lambert, P. & Bird, J. (2016a). Developing a measure to understand young children's Internet cognition and cyber-safety awareness: a pilot test. Early years. *British Journal of Educational Technology*, 36(3), 322– 335. https://doi.org/10.1080/09575146.2016.1193723.

Edwards, S., Nolan, A., Henderson, M., Skouteris, H., Mantilla, A., Lambert, P., & Bird, J. (2016b). Developing a measure to understand young children's internet cognition and cyber-safety awareness: a pilot test. *Early Years*, 36(3), 322–33,. https://doi.org/10.1080/09575146.2016.1193723.

Edwards, S., Nolan, A., Henderson, M., Mantilla, A., Plowman, L. & Skouteris, H. (2018). Young children's everyday concepts of the Internet: A platform for cyber-safety education in the early years. *British Journal of Educational Technology*, 49(1), 45–55. https://doi.org/10.1111/bjet.12529.

Englander., E. A. (2017). Children who own cell phones prone to cyberbullying. *Science and Children*, 55(3), 12–13.

eSafetyCommissioner. (2020). *Keeping children safe online during the covid-19 pandemic*. Retrieved 31 May 2020, from esafety.gov.au

Information and Computer Security

European Commission. (2018). *Safer Internet for the EU*. Retrieved 31 May 2020, from https://www.betterinternetforkids.eu/web/portal/saferinternet4eu

Ey, L.A. & Cupit, C. G. (2011). Exploring young children's understanding of risks associated with Internet usage and their concepts of management strategies. *Journal of Early Childhood Research*, 9(1), 53–65. https://doi.org/10.1177/1476718X10367471.

Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., & Collier, A. (2020). Youth internet safety education: aligning programs with the evidence base. *Trauma, Violence, & Abuse*, In Press. 1524838020916257.

Fleming, M. J., Greentree, S., Cocotti-Muller, D., Elias, K. A., & Morrison, S. (2006). Safety in cyberspace: Adolescents' safety and exposure online. *Youth & Society*, *38*(2), 135-154.

Franco, L., & Ghanayim, K. (2019). The Criminalization of Cyberbullying Among Children and Youth. Santa Clara Journal of International Law, 17(II), Article 2.

Frechette, J. (2005). Cyber-democracy or cyber-hegemony? Exploring the political and economic structures of the internet as an alternative source of information. *Library Trends*, 53(4), 555–575.

Gao, Z., Guo, H., Xie, Y., Luo, Y., Lu, H. & Yan, K. (2017). Childguard: A child-safety monitoring system. *IEEE MultiMedia*, 24(4), 48–57. https://doi.org/10.1109/MMUL.2017.4031309.

Geier, E. (2013). *Simple Steps to Protect Yourself on Public Wi-F*. Retrieved 27 May 2020, from https://www.pcworld.com/article/2042233/how-to-child-proof-the-internet.html

Ghazi, K. M. (2016). Safety and Security Measures in Egyptian Hotels. *Journal of Association of Arab Universities for Tourism and Hospitality*, 13(1), 165–190.

Giannakas, F. Kambourakis, G., Papasalouros, A., & Gritzalis, S. (2016). Security education and awareness for K-6 going mobile. *International Journal of Interactive Mobile Technologies (iJIM),* 10(2), 41–48.

GOV.UK. (2019). Teaching online safety in school. Retrieved 17 December 2020 from https://www.gov.uk/government/publications/teaching-online-safety-in-schools

Guan, J. & Huck, J. (2012). Children in the digital age: exploring issues of cybersecurity. In *Proceedings of the 2012 iConference*, pages 506–507. ACM.

Green, A., Wilkins, C., & Wyld, G. (2019). Keeping children safe online (Nominet). Retrieved 17 December 2020 from: www.thinkNPC.org

Grey, A. (2011). Cybersafety in early childhood education. Australasian *Journal of Early Childhood*, 36(2), 77–81. https://doi.org/10.1177/183693911103600210.

Gujjar, P. & Manjunatha, T. (2020). Technology Challenges in Social Networking and Cyber Security. In *Seventeenth AIMS International Conference on Management*, (pp. 822–825), Kozhikode, India.

Haddon, L. and Livingstone, S. (2012). *EU Kids Online: national perspectives*. Technical report, The London School of Economics and Political Science. Retrieved January 2021 from: http://eprints.lse.ac.uk/46878/

Halliday, J. (2019). *Thousands of children under 14 have been investigated by police for sexting*. Retrieved 30 Dec 2019, from https://www.theguardian.com/society/2019/dec/30/thousands-of-children-under-14-have-been-investigated-by-police-for-sexting

Halpert, B. (2010). Preschool information assurance curriculum development. In *Information Security Curriculum Development Conference*, (pp. 27–28), Kennesaw, Georgia. https://doi.org/10.1145/1940941.1940948

Hancock, M., Randall, R. & Simpson, A. (2009). From safety to literacy: Digital citizenship in the 21st century. *Threshold* www.ciconline.org/threshold.

Hanewald, R. (2008). Confronting the pedagogical challenge of cyber safety. *Australian Journal for Teacher Education*, 33(3), 1–16. https://doi.org/10.14221/ajte.2008v33n3.1.

Heider, K. (2015). Children and families in the information age. In K. Heider and M. Jalongo (Ed.), *Cybersafety in Early Childhood: What Parents and Educators Need to Know*, (pp. 277–292). Springer.

Information and Computer Security

Her Majesty's Government. (2019). *Online Harms White Paper*. Retrieved March 2020, from https://www.gov.uk/government/consultations/online-harms-white-paper

International Telecommunications Union (ITU). (2020) *Guidelines for industry on Child Online Protection*. Retrieved 17 December 2020 from: https://www.itu-cop-guidelines.com/industry

internetmatters.org. (2018). *Helping parents keep their children safe online*. Retrieved 31 May 2020, from https://www.internetmatters.org

Jadambaa, A., Thomas, H. J., Scott, J. G., Graves, N., Brain, D., & Pacella, R. (2019). Prevalence of traditional bullying and cyberbullying among children and adolescents in Australia: A systematic review and meta-analysis. *Australian & New Zealand Journal of Psychiatry*, 53(9), 878–888. https://doi.org/10.1177/ 0004867419846393.

Jensen, K. (2017). *Pedophiles Hunt Kids in Popular Gaming Chat Rooms*,. Retrieved 27 May 2020, from https://www.protectyoungminds.org/2017/08/10/pedophiles-hunt-kids-online/6

Jiow, H.J., & Lin, J. (2013). The influence of parental factors on children's receptiveness towards mobile phone location disclosure services. *First Monday*, 18(1). https://doi.org/10.5210/fm.v18i1.4284.

Kamath, M. (2018a). *Pen Test Partners*. Retrieved 27 May 2020, from https://www.techworm.net/2015/08/five-child-hackers.html

Kamath, M. (2018b). Meet these 5 child hackers who could become top cyber security researchers. https://www.techworm.net/2015/08/five-child-hackers.html

Kaspersky. (2019). *Internet Safety for Kids – Expert Advice for Connected Kids*. Retrieved 27 March 2020, from https://connectedkids.org.uk/connected-kids/

Kennedy, J. (2016). *ISPCC warning: 'cyber safety is the child protection issue of our time*'. Retrieved March 2020, from https://www.siliconrepublic.com/life/ispcc-cyber-safety-child-protection

Kimmel, S. (2018) *3 Ways To Block Kids From Installing Apps On Their Android Phone*. https://useboomerang.com/2018/07/25/3-ways-block-kids-installing-apps-android-phone/

Klaper, D. & Hovy, E. A taxonomy and a knowledge portal for cybersecurity. In *Proceedings of the 15th Annual International Conference on Digital Government Research*, (pp. 79–85), Aguascalientes, Mexico, 2014.

Kritzinger, E. (2016). Short-term initiatives for enhancing cyber-safety within South African schools. *South African Computer Journal*, 28(1), 1–17. http://doi.org/10.18489/sacj.v28i1.369.

Kritzinger, E. (2017a). Cultivating a cyber-safety culture among school learners in South Africa. *Africa Education Review*, 14(1), 22–41. https://doi.org/10.1080/18146627.2016. 1224561.

Kritzinger, E. (2017b). Growing a cyber-safety culture amongst school learners in South Africa through gaming. *South African Computer Journal*, 29(2), 16–35. https://doi.org/10.18489/sacj.v29i2.471.

Kritzinger, E., Bada, M. & Nurse, J.R.C. (2017). A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. *In IFIP World Conference on Information Security Education*, (pp. 110–120). Springer.

Kuss, D.J. and Griffiths, M.D. (2012) Online gaming addiction in children and adolescents: A review of empirical research. *Journal of Behavioral Addictions*, *1*(1), pp.3-22.

Larson, S. (2015). The cyber security fair: An effective method for training users to improve their cyber security behaviors. *Information Security Education Journal*, 2(1), 11–19.

Lastdrager, E., Gallardo, I. C., Hartel, P., & Junger, M. (2017). How effective is anti-phishing training for children? In *Thirteenth Symposium on Usable Privacy and Security* (SOUPS), (pp. 229–239).

Levine, E & Tamburrino, M. (2014). Bullying Among Young Children: Strategies for Prevention. Early *Childhood Educ Journal*, 42, 271–278. https://doi.org/10.1007/s10643-013-0600-y.

Li, Q. (2007). Bullying in the new playground: Research into cyberbullying and cyber victimisation. *Australasian Journal of Educational Technology*, 23(4), 435–454. https://doi.org/10.14742/ajet.1245.

Livingstone, S., Stoilova, M. & Nandagiri, R. (2019). *Talking to children about data and privacy online: research methodology*. Retrieved 11 November 2019, from

Information and Computer Security

http://eprints.lse.ac.uk/101284/1/Livingstone_talking_to_children_about_data_published.pdf Retrieved 11 November 2019.

Livingstone, A., Mascheroni, G., Ólafsson, K. & Haddon, L. (2014). *Children's online risks and opportunities: Comparative findings from EU Kids Online and Net Children Go Mobile*. Retrieved 15 November 2020 from eprints.lse.ac.uk/60513/

Livingstone, S. & Bober, M. (2004). UK children go online : surveying the experiences of young people and their parents [online]. London: LSE Research Online. Retrieved 17 December 2020 from: http://eprints.lse.ac.uk/archive/00000395

Livingstone, S., Davidson, J. & Bryce, J. (2017). Children's online activities, risks and safety A literature review by the UKCCIS Evidence Group. UK Council for Child Internet Safety. Retrieved 17 December 2020 from: https://www.lse.ac.uk/business-and-consultancy/consulting/assets/documents/childrens-online-activities-risks-and-safety.pdf

Lomas, N. (2018). *Call for smart home devices to bake in privacy safeguards for kids*. Retrieved 27 May 2020, from https://techcrunch.com/2018/09/18/call-for-smart-home-devices-to-bake-in-privacy-safeguards-for-kids/

Lorenz, B., Kikkas, K. & Osula, K. (2018). Development of Children's Cyber Security Competencies in Estonia. In *International Conference on Learning and Collaboration Technologies*, (pp. 473–482). Springer, Las Vegas, NV.

Mackey, T. K. & Nayyar, G. (2016). Digital danger: a review of the global public health, patient safety and cybersecurity threats posed by illicit online pharmacies. *British Medical Bulletin*, 118(1), 110–126. https://doi.org/10.1093/bmb/ldw016.

Marcoux, E. (2010). Cybersecurity and school libraries. *Teacher Librarian*, 2, 67–68.

Martellozzo, E., Monaghan, A., Davidson, J., & Adler, J. (2020). Researching the Affects That Online Pornography Has on UK Adolescents Aged 11 to 16. *SAGE Open*, *10*(1), 2158244019899462.

Martin, N. & Rice, J. (2012). Children's cyber-safety and protection in Australia: An analysis of community stakeholder views. *Crime Prevention and Community Safety*, 14(3), 165–181. https://doi.org/10.1057/cpcs.2012.4.

Martzoukou, K. (2020). "Maddie is online": an educational video cartoon series on digital literacy and resilience for children. *Journal of Research in Innovative Teaching & Learning*. In Press. DOI 10.1108/JRIT-06-2020-0031

Mason, M. (2010). Sample size and saturation in PhD studies using qualitative interviews. *Methods for Qualitative Management Research in the Context of Social Systems Thinking*, 11(3). https://doi.org/10.17169/fqs-11.3.1428

McGrew, S., Ortega, T., Breakstone, J., & Wineburg, S. (2017). Bigger than fake news. *American Educator*, 41(3), 4–9.

Meyer, Marisa, Victoria Adkins, Nalingna Yuan, Heidi M. Weeks, Yung-Ju Chang, and Jenny Radesky. Advertising in young children's apps: A content analysis. *Journal of Developmental & Behavioral Pediatrics* 40(1), 32-39.

Meyers, E. M., Nathan, L. P. & Unsworth, K. (2010). Who's watching your kids? Safety and surveillance in virtual worlds for children. *Journal for Virtual Worlds Research*, 3(2). https://doi.org/10.4101/jvwr.v3i2.1890.

Miles, M. B., & Huberman, A. M. (1984). Qualitative data analysis: A sourcebook of new methods. In *Qualitative data analysis: a sourcebook of new methods*. Sage publications.

Milosevic, T. & Livingstone, S. (2017). *Protecting children online? Cyberbullying policies of social media companies*. MIT Press, London, UK.

Mishna, F. Saini, M. & Solomon, S. (2009). Ongoing and online: Children and youth's perceptions of cyber bullying. *Children and Youth Services Review*, 31(12), 1222–1228. https://doi.org/10.1016/j.childyouth.2009.05.004.

Mishna, F., Cook, C., Saini, M., Wu, M.J. & MacFadden, R. (2011). Interventions to prevent and reduce cyber abuse of youth: A systematic review. *Research on Social Work Practice*, (1), 5–14. https://doi.org/10.1177/1049731509351988.

Morrow, P. J. (2018). The new age of cybersecurity privacy, criminal procedure and cyber corporate ethics. *Journal of Cybersecurity Research*, 3(1), 19–28. https://doi.org/10.19030/jcr.v3i1.10241.

Morse, J. M. (2016). Mixed method design: Principles and procedures (Vol. 4). Routledge.

Information and Computer Security

Moseley, K. L., Freed, G. L., & Goold, S. D. (2011). Which sources of child health advice do parents follow?. Clinical pediatrics, 50(1), 50-56.

Moye, D. (2015). *Talking Doll Cayla Hacked to Spew Filthy Things* (UPDATE). Retrieved 27 May 2020 from https: //www.huffingtonpost.co.uk/entry/my-friend-cayla-hacked_n_6647046

Murray, S. (2018). Safeguarding children and young people in the online environment: Safeguarding implications in respect of sexting and associated online behaviour. *J Nurs Res Pract*, 2(2), 26–29.

Mutula, S. M. (2008). Cyber security of children: Implications for Sub-Saharan Africa. In *Security and Software for Cybercafés*, (pp. 46–61). IGI Global.

Muir, K. & Joinson, A. (2020). An exploratory study into the negotiation of cyber-security within the family home. *Frontiers in Psychology*, 11, 424. https://doi.org/10.3389/fpsyg.2020.00424.

Nandhini, P. & Moorthi, K. (2018). A research on child safety wearable devices. *International Journal of AdvancedResearch*, 6(Oct),231-237. https://doi.org/10.21474/IJAR01/7804

Naidoo, T., Kritzinger, E., & Loock, M. (2013). Cyber safety education: towards a cyber-safety awareness framework for primary schools. In *International Conference on e-Learning*, (pp. 272). Academic Conferences International Limited.

Nairn, A. (2008). "It does my head in... buy it, buy it, buy it!" The commercialisation of UK children's web sites. *Young Consumers*. 9(4), 239-253. https://doi.org/10.1108/17473610810920461.

Nash, V. (2019). Revise and resubmit? Reviewing the 2019 Online Harms White Paper. *Journal of Media Law*, *11*(1), 18-27.

netsanity. (2017). *The Dangers for Children on Social Media*. Retrieved 27 May 2020, from https://netsanity.net/dangers-children-social-media-shocking/

Nield, D. (2018). *How to child-proof the Internet*. Pen Test Partners. Retrieved 27 May 2020., from https://www.wired.com/story/public-wifi-safety-tips/

NSPCC. (2020). Online Safety. Retrieved 17 December 2020 from: https://www.nspcc.org.uk/keeping-children-safe/online-safety/

OfCom. 2019. Children and parents: Media use and attitudes report 2019. Retrieved January 2021 from: https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2019

Ofcom. (2020). Internet users' experience of potential online harms: summary of survey research. Retrieved 17 December from https://www.ofcom.org.uk/research-and-data/internet-and-on-demand-research/internet-use-and-attitudes/internet-users-experience-of-harm-online

Olmstead, K. & Smith, A. (2017). Americans and cybersecurity. *Pew Research Center*, 26, 311–327.

Parker, D. (1999). Criteria for evaluating the condition of the tropical cyclone warning system. Disasters, 23 (3) 193-216.

Parris, L. N., Varjas, K. & Meyers, J. (2014) "The Internet is a Mask": High School Students' Suggestions for Preventing Cyberbullying. *Western Journal of Emergency Medicine*, 15(5), 587–592. https://doi.org/10.5811/westjem.2014.4.20725.

Paul, S. & Rioux, L. (2015). Over 20 years of research into cybersecurity and safety engineering: a short bibliography. *Safety and Security Engineering*, 5, 335–349.

Pietre-Cambacédes, L. & Chaudet, C. (2010). The SEMA referential framework: Avoiding ambiguities between security and safety. *Int. Journal of Critical Infrastructure Protection*, 3(2), 55-66. https://doi.org/10.1016/j.ijcip.2010.06.003

Price, E. (2020). *How to Try Microsoft's New Family Safety App*. Retrieved 27 May 2020, from https://offspring.lifehacker.com/how-to-try-microsofts-new-family-safety-app-1843479655

Prince, M. (2020). *Introducing 1.1.1.1 for Families*. Retrieved March 2020, from https://blog.cloudflare.com/introducing-1-1-1-1-for-families/

Information and Computer Security

Prior, S. & Renaud, K. (2020). Age-Appropriate Password "Best Practice" Ontologies for Early Educators and Parents. *International Journal of Child-Computer Interaction*. https://doi.org/10.1016/j.ijcci.2020.100169.

Pusey, P. & Sadera, W. A. (2011). Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education*, 28(2), 82–85. https: //www.learntechlib.org/p/55498/.

Quayle, E. (2020). Prevention, disruption and deterrence of online child sexual exploitation and abuse. In *ERA Forum* (pp. 1-19). Springer Berlin Heidelberg.

Rahman, N. R. A., & Abidin, Z. M. Z. (2019). A study on cyber safety awareness among Malaysian primary students a case study: QR code game in SK Bangi. *International Journal of Psychosocial Rehabilitation*, 23(4), 1343-1354. https://doi.org/10.37200/IJPR/V23I4/PR190460.

Razak, S. A. (2016). Aiming for cyber safety. *ITNOW*, 58(4), 34–35.

Renaud, K. & Van Biljon, J. (2019). A Framework to Maximise the Communicative Power of Knowledge Visualisations. SAICSIT Skukuza, South Africa, 17-18 September.

Renaud, K. & Prior, S. (2020). Children's password-related books: Efficacious, vexatious and incongruous, 2020. *Early Childhood Education Journal*. https://doi.org/10.1007/s10643-020-01067-z

Roberto, A. J., Eden, J., Savage, M. W., Ramos-Salazar, L. & Deiss, D. M. (2014). Outcome evaluation results of school-based cybersafety promotion and cyberbullying prevention intervention for middle school students. *Health Communication*, 29(10), 1029– 1042. https://doi.org/10.1080/10410236.2013.831684.

Rubenking, N. J. (2020). *The Best Free Antivirus Protection for 2020*. Retrieved March 2020, from https://uk.pcmag.com/antivirus/120817/the-best-free-antivirus-protection

Ruckelshaus, W.D., (1983). Science, risk, and public policy. *Science*, *221*(4615), 1026-1028.

SafeKids.com. *Kids' rules for online safety*, 2020. Retrieved 14 December 2019, from https://www.safekids.com/kids-rules-for-online-safety/.

Salim, H. & Madnick, S. (2016). *Cyber safety: A systems theory approach to managing cyber security risks–applied to TJX cyber attack*. Technical report, Sloan School of Management, MIT. Retrieved January 2021 from: https://cams.mit.edu/wp-content/uploads/2016-09.pdf

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students*. Pearson Education Limited. Essex, UK.

Shariff, S. (2008). *Cyber Bullying*. Routledge, New York, NY.

Shariff, S & Gouin, R. (2005), *Cyber-dilemmas: Gendered hierarchies, free expression and cyber-safety in schools*. In Oxford Internet Institute conference at Oxford University, Oxford, UK, pp. 147-154. Retrieved 29 December 2019

Shin, W., & Lwin, M. O. (2017). How does "talking about the Internet with others" affect teenagers' experience of online risks? The role of active mediation by parents, peers, and school teachers. *New Media & Society*, *19*(7), 1109-1126.

Shillair, R. (2016) Talking about online safety: A qualitative study exploring the cybersecurity learning process of online labor market workers. In *Proceedings of the 34th ACM International Conference on the Design of Communication*, (pp. 1–9).

Shneiderman, B. (1996). The eyes have it: A task by data type taxonomy for information visualizations. In *Proceedings 1996 IEEE symposium on visual languages*, (pp. 336–343). IEEE.

Slavtcheva-Petkova, V., Nash, V. J. & Bulger, M. (2015) Evidence on the extent of harms experienced by children as a result of online risks: implications for policy and research, *Information, Communication & Society*, 18:1, 48-62, DOI: 10.1080/1369118X.2014.934387

Stone, K. (2013). *Keeping children and young people safe online: balancing risk and opportunity*. WithScotland.Org Retrieved 24 March 2020, from https://docplayer.net/25298756-Keeping-children-and-young-people-safe-online-balancing-risk-and-opportunity.html

Information and Computer Security

Symons, K., Ponnet, K., Emmery, K., Walrave, M., & Heirman, W. (2017). Parental knowledge of adolescents' online content and contact risks. *Journal of Youth and Adolescence*, *46*(2), 401-416.

Tambini, D. (2019). The differentiated duty of care: a response to the Online Harms White Paper. *Journal of Media Law*, *11*(1), 28-40.

TeachThought Staff (2017). *7 ways to prevent cyberbullying*. Retrieved 27 May 2020, from https://www.teachthought.com/technology/7-ways-to-prevent-cyberbullying/

ThinkUKnow. (undated-a). *Help your children get the most out of the Internet*, Retrieved 31 May 2020, from https://www. thinkuknow.co.uk

ThinkUKnow. (undated-b). Teaching online safety in schools. Retrieved 17 December 2020 from: https://www.thinkuknow.co.uk/professionals/guidance/teaching-online-safety-in-schools/

Tonge, A. M., Kasture, S. S., & Chaudhari, S. R. (2013). Cyber security: challenges for society-literature review. *IOSR Journal of Computer Engineering*, 2(12), 67–75. https://doi.org/10.6084/m9.figshare.1104181.

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J. & Cotton, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, 59:138–150. https://doi.org/10.1016/j.cose.2016.02.009.

Tsatsanashvili, M. (2018). Juveniles safety on the internet in georgia (problems and methods of solution). *Bulletin of the Georgian National Academy of Sciences*, 12(1), 188–196.

Tsirtsis, A., Tsapatsoulis, N., Stamatelatos, M., Papadamou, K. & Sirivianos, M. (2016). Cyber security risks for minors: a taxonomy and a software architecture. In *IEEE 11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP)*, (pp. 93–99). IEEE, Thessaloniki, Greece.

UK Council for Internet Safety. (2020a). *Online safety*. Retrieved 31 May 2020, from https://www.nspcc.org.uk/keeping-children-safe/online-safety/

UK Council for Internet Safety. (2020b). *Net aware*. Retrieved 31 May 2020, from https://www.net-aware.org.uk

UK Council for Internet Safety. (2016). *Child safety online: A practical guide for parents and carers whose children are using social media*. Retrieved 31 May 2020, from https://www.gov.uk/ government/publications/child-safety-online-a-practical-guide-for-parents-and-carers/child-safety-online-a-practical-guide-for-parents-and-carers-whose-children-are-using-social-media

UNITED NATIONS. (2015). A call for an empowering, inclusive and safe digital environment for children. Retrieved 17 December 2020 from: https://www.ohchr.org/EN/Issues/Children/Pages/SafeDigitalEnvironment.aspx

UNICEF. (2019). Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry. Retrieved 21 June 2020 from: https://www.unicef- irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf

UNICEF. (2014). Guidelines for Industry on Child Online Protection. Retrieved 17 December 2020 from: https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf

Valcke, M., De Wever, B., Van Keer, H., & Schellens, T. (2011). Long-term study of safe Internet use of young children. *Computers and Education*, 57(1), 1292–1305. https://doi.org/10.1016/j.compedu.2011.01.010.

Vasiliev, Y.S., Zegzhda, P.D. & Kuvshinov, V.I. (2014). Modern problems of cybersecurity. *Nonlinear Phenomena in Complex Systems*, 17(3), 210 – 214.

Van Biljon, J. & Renaud, K. Facilitating knowledge visualisation as communication and knowledge transfer mechanism in postgraduate learning. In *International Conference on Mobile and Contextual Learning*, (pp. 156–171). Springer, Cham, 2015. https://doi.org/ 10.1007/978-3-319-25684-9_12.

Van Niekerk, J. Thomson, K.L., & Reid, R. (2009). Cyber safety for school children. In *Information Security Education*, (pp. 103–112), Berlin, Heidelberg, 2009. Springer.

Information and Computer Security

Van Niekerk, J., Thomson, K-L. & Reid, R. (2013). Cyber safety for school children: a case study in the Nelson Mandela metropolis. *International Federation for Information Processing Publication - IFIP*, 1(406), 103–112. https://doi.org/10.1007/978-3-642-39377- 8_11.

Van Ouytsel, J., Walrave, M. & Van Gool, E. (2014). Sexting: Between thrill and fear — How schools can respond. *The Clearing House: A Journal of Educational Strategies, Issues and Ideas*, 87(5), 204–212.

Von Solms, S. and Von Solms, R. (2014). Towards Cyber Safety Education in Primary Schools in Africa. In *HAISA*, Plymouth, UK. (pp. 185–197).

Von Solms, R. & Von Solms, S. (2015). Cyber safety education in developing countries. *International Institute of Informatics and Systemics*. 13(3), 14-19. Retrieved 14 Dec 2019, from https://www.iiisci.org/journal/CV$/sci/pdfs/EA940GX15.pdf

Walker, L. (2017). The Porn Harms Kids Report. Retrieved 17 December 2020 from: http://www.academia.edu/download/62257355/Porn_Harms_Kids_Full_Report_25.9.1720200302-123244-4og3uh.pdf

Wayman, S. (2017). *Why teaching children about cyber safety at eight is too late*. Retrieved 28 March 2020, from https://www.irishtimes.com/life-and-style/health-family/parenting/why-teaching-children-about-cyber-safety-at-eight-is-too-late-1.2906323.

Ward, K., & Hawthorne, K. (1994). Do patients read health promotion posters in the waiting room? A study in one general practice. *British Journal of General Practice*, 44(389), 583-585.

Wilson, J. (2020). Online child abuse rises to 90 recorded incidents a day. E&T (Engineeering and Technology). Retrieved 17 December 2020 from: https://eandt.theiet.org/content/articles/2020/01/online-abuse-crimes-against-children-rise-to-90-recorded-incidents-a-day-nspcc-estimates/

Xu, z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM*, 56(4), 64–74.

Zepf, Arthur, L. (2013). *Cyber-security curricula for basic users*. Master's thesis, NAVAL POST-GRADUATE SCHOOL MONTEREY CA, 2013. Masters Dissertation, School of Computer Science.

Information and Computer Security

Table 2: Examples of risky online actions from the literature

Risky Behaviour	**Sources**	**Potential Harm Example**
H1: Sharing personal information	Van Niekerk *et al.*, 2009, Von Solms and Von Solms, 2015, Dooley *et al.*, 2009, UK Council for Internet Safety, 2020a, Morrow, 2018, Hancock *et al.*, 2009, Dooley *et al.*, 2009, Kritzinger, 2017b, Conroy, 2007.	Identity theft Child at risk of being contacted
H2: Accessing harmful content online	Her Majesty's Government, 2019, Heider, 2015b, UK Council for Internet Safety, 2020a, Christensen and Aldridge, 2012, Boyd, Marwick, Aftab, and Koeltl, 2009, Kritzinger, 2017b, Valcke, De Wever, Van Keer, and Schellens, 2011, European Commission, 2018, Livingstone, Davidson and Bryce, 2017.	Self harm, radicalisation
H3: Consuming misinformation	Valcke *et al.*, 2011, European Commission, 2018, McGrew, Ortega, Breakstone, and Wineburg, 2017.	Engaging in harmful challenges; Self Harming
H4: Device Discloses Realtime Location Device Discloses Realtime Location	Jiow and Lin, 2013.	Child could be tracked by unknown adult
H5: Divulging Passwords	Choong *et al.*, 2019, Van Niekerk *et al.*, 2009, Agarwal and Singhal, 2017.	Impersonation
H6: Becoming Addicted to Computers	Christensen and Aldridge, 2012, Conroy, 2007.	Not developing social skills and becoming reclusive
H7: Unwise Downloads	DeFranco, 2011, Kritzinger, 2016.	Device getting Infected with a Virus;
H8: Engaging in cyber violence including cyber bullying	Hancock *et al.*, 2009, Van Niekerk *et al.*, 2009, Agarwal and Singhal, 2017, Mishna *et al.*, 2009, Paunovíc, 2018, Jadambaa *et al.*, 2019, UK Council for Internet Safety, 2020a, Kritzinger, 2017b, European Commission, 2018, Conroy, 2007, Shariff, 2008, Shariff and Gouin, 2005, Mishna, Cook, Saini, Wu, and MacFadden, 2011, Li, 2007, Levine and Tamburrino, 2014, Livingstone,	Mental health issues

Information and Computer Security

	Davidson and Bryce, 2017; Slavtcheva-Petkova, Nash and Bulger, 2015.	
H9: Sexting	Kritzinger *et al.*, 2017, UK Council for Internet Safety, 2020a, European Commission, 2018, Conroy, 2007, Mishna *et al.*, 2011, Murray, 2018, Halliday, 2019, Livingstone, Davidson and Bryce, 2017; Slavtcheva-Petkova, Nash and Bulger, 2015.	Blackmail and shaming
H10: Cyber grooming, cyberstalking, sexual solicitation, adults pretending to be children	Hancock *et al.*, 2009, Van Niekerk *et al.*, 2009, Dooley *et al.*, 2009, Boyd *et al.*, 2009, Valcke *et al.*, 2011, European Commission, 2018, Conroy, 2007, Mishna *et al.*, 2011, Hanewald, 2008, Stone, 2013, Ey and Glenn Cupit, 2011.	Adults trying to meet children in the physical world
H11: Being targeted by advertising	Dooley *et al.*, 2009, UK Council for Internet Safety, 2020a, Kritzinger, 2016, Livingstone, Davidson and Bryce, 2017.	Child feels pressured to buy things; Mental health issues
H12: Use of Public WiFi	Lorenz *et al.*, 2018, Meyers, Nathan, and Unsworth, 2010.	Information leaked and possibly abused
H13: Falling for a Phishing Message	Muir and Joinson, 2020, Agarwal and Singhal, 2017, Lastdrager *et al.*, 2017, DeFranco, 2011, Al Shamsi, 2019.	Someone knowing the child's password Malware installed on device

Table 3: New Risky Behaviours that Emerged from the Focus Groups

Risky Behaviour	**Source**	**Potential Harm**
H14: Smart toys being hacked	European Commission, 2018, Moye, 2015.	Hackers exposing child to adult content Hackers contacting the child
H15: Children "hacking" each other i.e. guessing passwords or persuading others to share their passwords	Kamath, 2018a.	Digital items being stolen
H16: Children using social media before the mandated age	netsanity, 2017.	Seeing disturbing content Being contacted by adults online
H17: Smart assistants in the home not being child friendly	Lomas, 2018.	Child being exposed to adult content Child ordering goods from online store

Information and Computer Security

Table 4: Ages at which children are likely to engage in specific risky behaviours

4-8	H5: Divulging Passwords (Prior and Renaud, 2020) H2: Accessing harmful content online (Ofcom, 2019) H11: Being targeted by advertising (Meyer *et al.*, 2019) H3: Consuming misinformation (Ofcom, 2019) H4: Device Discloses Realtime Location Device Discloses Realtime Location (Ofcom, 2019) H17: Smart assistants in the home not being child friendly (Ofcom, 2019) H14: Smart toys being hacked (Ofcom, 2019)
8-10	H15: Children "hacking" each other i.e. guessing passwords or persuading others to share their passwords (Kamath, 2018b). H6: Becoming Addicted to Computers (Kuss and Griffiths, 2012) H7: Unwise Downloads (Kimmel, 2018) H10: Cyber grooming, cyberstalking, sexual solicitation, adults pretending to be children (Davidson *et al.*, 2011) H12: Use of Public WiFi (Ofcom, 2019) H13: Falling for a Phishing Message (Lastdrager *et al.*, 2017) H16: Children using social media before the mandated age (Haddon and Livingstone, 2012)
10+	H8: Engaging in cyber violence including cyber bullying (Hanewald, 2008) H9: Sexting (Davidson *et al.*, 2017; Comartin *et al.*, 2013). H1: Sharing personal information (Chappell, 2012)

Information and Computer Security

Table 5: Mapping Risky Activities to Counter-Measures

	Mentor	**Mitigate**	**Monitor**
H1	Jensen (2017)		
H2	Her Majesty's Government (2019)	UK Council for Internet Safety (2020b), Prince (2020)	Geier (2013)
H3	Her Majesty's Government (2019)	UK Council for Internet Safety (2020b), Prince (2020)	Geier (2013)
H4	common sense media (undated-a)		
H5	Prior and Renaud (2020)		
H6	Her Majesty's Government (2019)	Geier (2013)	Geier (2013)
H7		Barbara (2020)	
H8	Her Majesty's Government (2019), TeachThought Staff (2017)		
H9	Van Ouytsel, Walrave, and Van Gool (2014), Döring (2014)		
H10	Jensen (2017)		Jensen (2017)
H11	Nairn (2008)	Cook (2019), Attached Mama (2009)	
H13	Nield (2018)	Child Safe VPN (2020)	
H14	Lastdrager *et al.* (2017)	Rubenking (2020)	
H15		Choi (2018)	
H16	Xu, Hu, and Zhang (2013)		
H17	Her Majesty's Government (2019)		Price (2020)
H18		Munro (2019)	

Information and Computer Security